“网络空间安全治理”重点专项2022年度项目申报指南

申报资格要求

1. 项目牵头申报单位和参与单位应为中国大陆境内注册的科研院所、高等学校和企业等，具有独立法人资格，注册时间为2021年6月30日前，有较强的科技研发能力和条件，运行管理规范。国家机关不得牵头或参与申报。

项目牵头申报单位、参与单位以及团队成员诚信状况良好，无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

申报单位同一个项目只能通过单个推荐单位申报，不得多头申报和重复申报。

2. 项目（课题）负责人须具有高级职称或博士学位，1962年1月1日以后出生，每年用于项目的工作时间不得少于6个月。

3. 项目（课题）负责人原则上应为该项目（课题）主体研究思路的提出者和实际主持研究的科技人员。中央和地方各级国家机关的公务人员（包括行使科技计划管理职能的其他人员）不得申报项目（课题）。

4. 项目（课题）负责人限申报1个项目（课题）；国家科技重大专项、国家重点研发计划、科技创新2030—重大项目的在研项目负责人不得牵头或参与申报项目（课题），课题负责人可参与申报项目（课题）。

项目（课题）负责人、项目骨干的申报项目（课题）和国家科技重大专项、国家重点研发计划、科技创新2030—重大项目在研项目（课题）总数不得超过2个。国家科技重大专项、国家重点研发计划、科技创新2030—重大项目的在研项目（课题）负责人和项目骨干不得因申报新项目而退出在研项目；退出项目研发团队后，在原项目执行期内原则上不得牵头或参与申报新的国家重点研发计划项目。

项目任务书执行期（包括延期后的执行期）到2022年12月31日之前的在研项目（含任务或课题）不在限项范围内。

5. 参与重点专项实施方案或本年度项目指南编制的专家，原则上不能申报该重点专项项目（课题）。

6. 受聘于内地单位的外籍科学家及港、澳、台地区科学家可作为项目（课题）负责人，全职受聘人员须由内地聘用单位提供全职聘用的有效材料，非全职受聘人员须由双方单位同时提供聘用的有效材料，并作为项目预申报材料一并提交。

7. 申报项目受理后，原则上不能更改申报单位和负责人。

8. 项目具体申报要求详见各申报指南，有特殊规定的，从其规定。

各申报单位在正式提交项目申报书前可利用国科管系统查询相关科研人员承担国家科技重大专项、国家重点研发计划重点专项、科技创新2030—重大项目在研项目（含任务或课题）情况，避免重复申报。

其他内容请详见通知内容及附件。

附件列表

序号	附件名称	操作
1	“网络空间安全治理”重点专项2022年度项目申报指南.pdf	查看　下载
2	“网络空间安全治理”重点专项2022年度项目申报指南形式审查条件要求.pdf	查看　下载
3	科技部关于发布国家重点研发计划“先进结构与复合材料”等重点专项2022年度项目申报指南的通知.pdf	查看　下载

附件 17

"网络空间安全治理"重点专项 2022 年度项目申报指南

为落实"十四五"期间国家科技创新有关部署安排，国家重点研发计划启动实施"网络空间安全治理"重点专项。根据本重点专项实施方案的部署，现发布 2022 年度项目申报指南。

本重点专项总体目标是：围绕全球网络公害、涉及民生的数据资产和"新基建"基础设施等领域的安全挑战，开展互联网基础设施、数据、网络公害、新技术新应用领域安全治理的战略性、基础性、前沿性研究，到 2025 年力争打造自立自强的网络空间安全治理技术体系，形成中国特色的网络空间安全治理方案，支撑实现网络空间的"共建、共治、共享"。

2022 年度指南部署坚持问题导向、分步实施、重点突出的原则，围绕互联网基础设施治理、网络空间数据治理、网络公害与内容治理、新技术新应用治理 4 个技术方向，按照基础研究、共性关键技术等层面，拟启动 26 项指南任务，拟安排国拨经费 3.66 亿元。其中，围绕互联网基础设施治理、网络空间数据治理、网络公害与内容治理等技术方向，拟部署 5 个青年科学家项目，拟安排国拨经费 1000 万元，每个项目 200 万元。除基础研究类项目外，配套经费与国拨经费比例不低于 1:1。

项目统一按指南二级标题（如 1.1）的研究方向申报。除特殊说明外，每个方向拟支持项目数为 1~2 项，实施周期不超过 3 年。申报项目的研究内容必须涵盖二级标题下指南所列的全部研究内容和考核指标。基础研究类项目下设课题不超过 4 个，项目参与单位总数不超过 6 家；共性关键技术类项目下设课题数不超过 5 个，项目参与单位总数不超过 10 家。项目设 1 名项目负责人，项目中每个课题设 1 名课题负责人。

青年科学家项目不再下设课题，项目参与单位总数不超过 3 家。项目设 1 名项目负责人，青年科学家项目负责人年龄要求，男性应为 1984 年 1 月 1 日以后出生，女性应为 1982 年 1 月 1 日以后出生。原则上团队其他参与人员年龄要求同上。

指南中"拟支持数为 1~2 项"是指：在同一研究方向下，当出现申报项目评审结果前两位评价相近、技术路线明显不同的情况时，可同时支持这 2 个项目。2 个项目将采取分两个阶段支持的方式。第一阶段完成后将对 2 个项目执行情况进行评估，根据评估结果确定后续支持方式。

1. 基础研究类

1.1 分布式学习中的数据安全基础理论

研究内容：针对分布式学习系统在充分释放海量数据价值过程中存在的数据泄露、模型篡改、模型窃取等攻击行为，研究分布式学习场景下数据安全的基础理论框架；研究分布式学习场景下训练数据筛选与过滤技术；研究面向模型训练阶段的隐私保护

技术；研究面向模型预测阶段的隐私保护技术；研究分布式场景下学习模型的安全性验证技术。

考核指标：突破基于敏感数据的模型训练与预测技术，支持不少于 3 种常见开发框架与 5 种常见学习算法；按照密码学和安全领域规范定义系统和安全模型，明确安全假设，给出系统化的安全分析；实现密文态数据上的小时级模型训练与秒级预测，模型参数规模不低于百万级，密文态数据上的模型预测精确度下降不超过 3%；实现基于混淆扰动的模型分布式训练，模型预测的精确度下降不超过 3%；实现抗篡改、窃取等攻击行为的模型分布式训练，检测攻击的成功率超过 98%，模型预测的精确度下降不超过 5%。

1.2 网络空间与自然社会安全行为协同关联理论（青年科学家项目）

研究内容：研究网络空间中的个体身份、群体结构与社团、群体复杂关系和行为模式分析理论和方法，突破网络空间中时空动态社会安全行为理解的技术瓶颈；研究跨平台动态可扩展的网络身份行为标准表征技术；研究人物关系图谱交互式构建和智能推理技术，实现网络空间虚拟身份特征与实体特征表达的映射；研制网络空间与自然社会安全行为协同关联分析原型系统。

考核指标：支持不低于三种网络空间实体对象的身份表达类型，支持亿级以上网络空间实体对象的身份检测模型和算法，多

模态身份检测准确率不低于 85%；在千万级成员规模下，网络空间实体对象的身份检测准确率不低于 80%；成员的检测准确率在典型公开数据集上准确度不低于 70%；支持不同长度的时间窗口下的行为模式挖掘和最低 6 种社会活动类型识别，已知社会结构识别准确率不低于 90%，未知社会结构识别准确率不低于 75%；支持千万级规模人物关系图谱中的隐关系推理，推理精度达 75%以上；关键考核指标达到同期国际先进水平。

1.3 分布式非协作网络的可信访问和路径溯源方法

研究内容：针对分布式非协作网络环境下可信访问认证难、伪造流量识别难、用户身份追溯难的问题，研究基于加密签名的非协作网络间源地址验证机制，研究基于源地址验证表的非协作网络间源地址验证机制，研究轻量级转发路径验证和路径追溯机制，研究基于地址标签的终端身份认证机制。

考核指标：基于加密签名的非协作网络间源地址验证，支持层次化的密钥和标签管理，分布式密钥分发和管理达到与域内域间路由协议同等的收敛时间要求；基于源地址验证表的非协作网络间源地址验证，避免增量部署时报文误丢弃，支持虚拟专用网/隧道、分段路由等策略路由场景下的准确源地址验证；轻量级转发路径验证和路径追溯，通信开销和计算开销相比业界的 OPT 方案降低 50%，有效吞吐率达到 95%；基于地址标签的终端身份认证，具备单一域内不少于 10 万动态标签的管理和验证能力；相关研究成果达到同期国际先进水平。

1.4 数字身份密码协议的安全设计与分析理论（青年科学家项目）

研究内容：围绕数字经济发展下用户身份的隐私保护需求，研究基于密码学的数字身份协议及其密码组件化设计与分析理论；研究基于自主身份的访问控制协议；研究基于自主身份，可满足前向安全、已知密钥安全等安全属性的认证密钥协商协议。

考核指标：提出不少于 1 种基于密码学的数字身份协议组件的设计方法；设计不少于 1 套基于自主身份的访问控制协议，需支持细粒度身份属性表达与访问控制；设计不少于 1 套基于自主身份的认证密钥协商协议，满足前向安全、已知密钥安全等属性；关键考核指标达到同期国际先进水平；提交国家或行业标准提案不少于 1 项。

1.5 受限感知能力下社交网络虚假信息检测与溯源方法（青年科学家项目）

研究内容：针对虚假信息防控需求，分析虚假信息在不同类型社交网络内部与跨平台传播特性，建立典型社交网络平台虚假信息传播的动力学模型；研究社交网络结构特征对虚假信息传播的影响机理，设计面向信息传播的超大规模网络结构拆解算法；研究多模态虚假信息快速检测方法，并探索算法在有限检测资源、内容无法获取等受限感知能力下的扩展；研究跨时空社交网络虚假信息精准溯源技术，并探索算法在网络拓扑不完全等受限感知能力下的拓展。

考核指标：建立不少于 3 种典型社交网络的虚假信息传播模型；虚假信息检测准确率不小于 80%；设计超大规模网络拆解算法不小于 5 个，实现千万级网络拆解内存消耗不超过 64GB，计算时间不超过 10 分钟，综合性能优于 CI、FINDER 等主流算法；侦测典型网络高传播风险虚假信息所需监控的网络节点占比不高于 10%，发现时平均传播范围低于 1%；给定信息资源场景下的溯源定位源集不大于网络规模的 1%；关键考核指标达到同期国际先进水平。

1.6 基于智能博弈的网络安全风险主动发现与抑制机理（青年科学家项目）

研究内容：基于智能博弈理论，研究端网协同的网络安全新风险发现与识别技术；研究网络安全知识平面，突破端网、多体制网络之间的信息与互信壁垒，实现智能化网络安全风险的协同发现与主动防范；研究智能安全博弈协议，实现对网络安全未知风险的主动抑制和“易守难攻”的网络空间安全。

考核指标：突破端网协同的安全新风险发现与识别技术，支持 IP、5G、卫星等多体制、高动态网络/通信体制；提出网络安全知识平面，内置 3 种以上智能博弈机制激励端网、多体制网络间的互信构建与知识共享；针对 DDoS 等智能化恶意网络流量攻击，在攻击手段与漏洞未知的条件下，抑制最优攻击策略的攻击成本收益比趋于 0；相关研究成果达到同期国际先进水平。

1.7 网络空间内生安全机制与评估方法（青年科学家项目）

研究内容：提炼网络空间内生安全问题的共性特征，构建网络空间内生安全理论模型；在不依赖外部攻击者先验知识的条件下，提出解决内生安全问题的普适性方法，有效应对不确定性威胁；提出网络空间内生安全评估方法。

考核指标：建立一套网络空间内生安全理论模型；提出不少于 2 种的网络空间内生安全方法；能够抵御不少于 10 种攻击包括 0-day 漏洞和 APT 攻击等，成功率大于 90%；建立网络空间内生安全定性和定量的评估指标体系；关键考核指标达到同期国际先进水平。

2. 共性关键技术类

2.1 网络空间抗测绘关键技术

研究内容：针对网络空间测绘活动大量窃取网络关键信息、严重威胁关键信息基础设施安全的问题，研究网络空间抗测绘理论、模型及效能评估体系；研究可对抗网络扫描、网络设备指纹分析等网络测绘技术的理论与方法；研究保护关键节点与关键路径的抗测绘关键技术；研究网络空间测绘与网络空间抗测绘之间的对抗博弈关系及演化机制等，提出网络空间抗测绘动态演化方法。

考核指标：构建完整的网络空间抗测绘理论及评价体系，构建一个虚实结合的网络空间抗测绘验证环境；可对抗至少 3 种基于人工智能模型的网络设备识别方法，受保护设备正确识别成功率不高于30%，受保护设备类型包括路由交换设备、服务器和PLC

设备等网络关键设备；在常见拓扑信息探测方法下，受保护拓扑信息正确获取成功率不高于 30%；可对抗至少 3 种隐蔽网络扫描策略组合方法，受保护端口存活发现成功率不高于 30%；提出适应动态场景的网络空间测绘与网络空间抗测绘博弈演化模型。

2.2 域名递归解析服务的安全监管与治理技术

研究内容: 针对域名递归解析服务器广泛存在的劫持、篡改、信息泄露、被攻击利用等安全风险，研究递归解析服务器及其层级依赖关系、服务范围及服务质量的快速发现技术；研究递归解析服务器的风险建模、威胁发现、恶意行为分析和安全态势感知技术，评估递归解析服务器的安全状况及威胁影响范围；研究 DoH、DoT、DNSSEC 等 DNS 安全增强措施在递归解析服务器的部署态势；研究基于域名解析服务数据的大规模网络攻击发现及预警技术;研究应对上述安全风险的递归解析服务监管处置技术，支持恶意域名过滤与重要域名保全的监管需求。

考核指标: 递归解析服务监管及 DNS 安全增强措施部署监测，可覆盖国内主要的服务提供方,递归解析服务器数量达到 10 万级，具备对 DNS 安全增强措施错误部署的检测和告警能力；支持百万级重点域名的解析状况分析及解析异常发现;提出基于域名数据的大规模网络攻击风险发现模型;提出递归解析服务器的风险监管处置体系，具备针对各种安全风险的快速预警和响应能力。

2.3 重要数据分类、识别与安全评估技术

研究内容：落实《中华人民共和国数据安全法》等政策法规

要求，支撑国家重要数据安全监管目标，在数据分类分级制度下研究重要数据识别方法和各地区、各行业重要数据目录制定方法；研究重要数据特征识别提取技术和重要性评估技术，并建立重要性特征信息比对库；针对大规模机构中数据分散存储保管等情况，研究重要数据扫描发现技术；研究公共网络中重要数据发现、甄别与责任追究技术；针对重要数据违规流转、非法出境等问题，研究违法违规行为发现技术。

考核指标：形成 1 套重要数据识别规范；建立科技信息、医疗健康、地理测绘等 3~5 个领域的行业数据分类分级方案和重要数据具体目录编制方案；建立 1 套覆盖国家、地方、行业监管需求的重要数据目录上报平台原型系统；提取至少 10 种行业专有数据指纹特征，实现至少 10 类行业专用文件的重要性特征识别提取，并建立 3~5 个行业的重要性特征信息比对库，重要性判断时间在毫秒级；实现一套大规模分散存储保管条件下的重要数据扫描、登记原型系统；实现面向公共网络的至少 500 万条规模的数据重要性评估，排查至少 5 个行业数据源可靠性；研制重要数据违规流转和非法出境监测发现示范应用平台。

2.4 非受控环境下数据资产保护技术

研究内容：研究基于时间和位置属性的非受控环境下数据访问控制方法，实现非受控环境下数据细粒度的按时发布、密钥泄露的可追踪、数据访问的可留痕；研究数据动态鉴权、细粒度数据授权等技术，有效解决非受控环境下数据确权难题；研究云数

据细粒度清洗方法，满足用户对外包至非受控环境下的数据资产的安全需求及存储效率需求，避免数据泄露问题；研究非受控环境下数据操作可信管理方法，有效保护敏感数据，满足不同用户、不同应用、不同时间段等对非受控环境下海量数据删除、外发、拷贝、修改等细粒度确定性操作的需求；研究非受控环境下数据高效安全回传技术。

考核指标：研制非受控环境下数据资产保护示范应用平台，支持非受控环境下数据细粒度访问控制；500MB 大小文件数据去重时间保持秒级；设计支持至少 10TB 级的云数据可信删除方法及系统；研究开发测试验证工具，完善非受控环境下数据资产保护系统；具备完善的数据权限和账户管理功能，可支撑包括数据提供方、数据使用方的数据所有权和使用权界定，实现防溯源防追踪的数据高效安全回传。

2.5 大数据平台安全监管与治理技术

研究内容：针对大数据平台数据泄露、数据滥用等问题，研究大数据场景下的量化风险识别技术，全面衡量大数据平台安全风险状态；研究大数据场景下的隐私增强与效果验证技术，为大数据平台安全监管提供底层技术支撑；研究运行时行为感知与管控和风险控制技术，解决大数据平台管控与监管能力缺失的难题；研究数据驱动的运行后审计与攻击溯源技术，实现攻击可复现，可溯源，可取证；研发大数据监管平台，支持海量数据风险识别、运行时安全管控、运行后审计等功能。

考核指标：完成 1 套至少涵盖重标识攻击、差分攻击、统计推断攻击等三种典型攻击场景的大数据量化风险识别系统研制，具备支持 10 亿行、1000 维以上数据量化风险评估的能力，且量化风险评估时间不大于 8 小时；完成 1 套大数据安全监管系统研制，支持海量数据风险识别、运行时安全管控和运行后审计与风险控制，可根据风险识别和管控需求实时阻断大数据平台的计算与处理任务，系统所能支持的数据量级不低于 1PB；形成大数据平台安全监管实践，形成行业标准提案；在至少 2 个涉及 1 亿行以上数据的实际业务场景开展业务示范。

2.6 多媒体大数据的隐私保护技术

研究内容：针对图像、视频等典型多媒体大数据服务面临的安全和隐私威胁，以及海量多媒体数据处理效率与可用性方面的要求，研究多媒体大数据轻量级安全存储与共享技术；研究多媒体大数据查询服务中的高效验证与隐私保护技术；研究多媒体大数据发布中的隐私内容检测与保护技术;研究多媒体大数据视觉、语音听觉安全客观评价理论及分析方法；研究支持隐私保护的多媒体大数据处理与分析技术。

考核指标：建立 10 万张以上图像视觉安全测试数据库，设计至少 3 种常用的图像视觉安全评价指标，并给出形式化的安全性证明；研发自主可控的多媒体大数据安全存储系统，单命名空间文件数容量 100 亿以上，单机吞吐量 10Gb/s 以上，支持 TB 级多媒体数据的轻量级加密，加密时间开销比传统主流加密方法降

低 60%以上；实现千万级图像数据量的检索验证，验证时间在秒级以下；研制 1 套多媒体大数据隐私保护关键技术集成平台，并至少在一个行业的 TB 级数据集上进行应用。

2.7 网络开源多模态科技情报智能分析

研究内容：研究复杂网络条件下互联网开源数据稳定获取技术；研究多模态开源数据治理与融合链接技术、人物属性关系推理补全技术、虚拟身份关联技术、跨数据源的情报知识迭代校验方法；研究碎片化信息关联整合、多源异质科技情报信息网络构建技术，实现完整、高质量的科技情报信息网络构建和组织；研究多语言环境下数据内容识别与信息认知技术；研究情报智能推理与情报自动化加工技术。

考核指标：支持境内外社交媒体、新闻网络、信息站点、网络论坛等不少 200 种开源数据源的稳定获取；支持文本、图像、视频、音频等数据的融合处理；支持亿级实体规模的异质科技情报信息网络构建；支持中、英、西、俄等主要语种科技情报的自然语言处理、实体链接、属性抽取、关系抽取，准确率大于 80%；研制 1 套网络开源多模态大数据情报智能分析平台，在科技情报相关领域示范应用。

2.8 智能算法模型安全评估与风险监测技术

研究内容：面向互联网信息服务算法综合治理的国家需求和智能算法应用面临的透明可释、数据安全、模型可信、风险可控等技术需求，研究智能算法的脆弱性和归纳偏置等安全机理，形成人工

智能的内生安全基础理论；研究人工智能系统面临的攻防博弈机理，形成人工智能系统的自我学习和安全增强技术，建立智能算法主动安全基础理论，构建针对人工智能模型的攻防博弈平台；研究人工智能系统的数据安全机理，形成抗逆向工程技术和数据后门检测方法，构建数据安全检测工具集和评估标准；研究智能算法缺陷检测和安全评估技术，建立智能算法安全风险全流程分析方法，形成算法缺陷检测工具集和算法安全评估标准；研究智能算法风险产生和演变机理，构建支持智能算法运行时风险监测的沙箱测试平台；研制智能算法安全评估与风险监测示范应用平台，服务于智能信息时代国家网络空间安全治理能力的提升。

考核指标：建立算法基础谱系及安全威胁图谱，覆盖不少于100 类主流人工智能算法和模型；针对至少 1 种人工智能安全应用系统，建立不少于 3 种学习框架的攻防博弈平台；研制 1 套数据安全检测工具集，支持不少于 100 种攻击方法的检测，检测准确率不低于 90%，并提交至少 1 项数据安全评估标准；研制面向智能算法运行时风险监测的沙箱测试平台，支持数据收集、模型训练、决策推断等智能算法全流程风险监测，在 1000PFlops（每秒浮点运算次数）算力级别的国产超算平台部署并运行全流程风险监测实验；建立智能算法安全评估与风险监测示范应用平台，实现对 80%以上关键领域算法安全监测与评估，实现 3 个及以上省级节点部署，形成国家区域多级联动的国家级人工智能综合防御体系。

2.9 密码芯片信息泄漏深度分析与可靠防护关键技术

研究内容：围绕泛在信息泄漏互作用机理机制基础理论、安全验证模型、安全特征建模、新颖量化度量与可靠防护机制关键技术、技术概念验证原型 IP 核以及先进分析测评支撑工具环境研制等六个方面开展，研究密码芯片信息泄漏互作用机理机制；研究密码芯片信息泄漏融合分析方法；研究密码芯片信息泄漏风险威胁量化度量构造方法；研究密码芯片信息泄漏风险深度检测技术；研究基于形式验证和标准 EDA 工具的密码核设计安全性评估方法；研究密码芯片泛在信息泄漏可靠防御理论与系统设计方法；建立密码芯片安全测试与检测试验床等。

考核指标：在密码芯片信息泄漏互作用机理认知方面形成重要突破；形成密码芯片信息泄漏深度风险分析形式化模型和度量新手段，信息泄漏风险检测的误报率比现有广泛采用的测试向量泄漏评估方法至少降低 20%，检测出信息泄漏所需样本数量至少降低 20%；建立密码芯片信息泄漏可靠防御的新方法，可以抵抗经典侧信道攻击，特别是高级侧信道攻击方法；支持机密性属性的形式化验证，能够采用形式化验证手段实现密码核设计安全性的形式化证明和泄漏检测；面向国际密码算法，提出密码芯片安全设计新架构并研制 2~3 款技术概念验证原型 IP 核；研制密码芯片信息泄漏风险深度分析检测工具集，建立密码芯片安全测试与检测试验床等。

2.10 软件供应链安全风险分析与检测技术

研究内容：针对软件供应链面临的安全风险，研究软件供应

链全生命周期的安全风险分析模型，为制定相关管理规范提供技术支撑；研究软件产品与服务供应链组件、构成成分、依赖组件智能识别与关系图谱分析技术，软件供应链风险分析评价方法，构建供应关系图谱分析和风险评价能力；研究基于源码和二进制的软件缺陷分析、高危缺陷提前感知、组件缺陷关联分析技术，并提出缺陷定位和风险评估方案，形成相应的分析工具；研究软件识别技术，构建常见软件的网络特征图谱，实现软件识别和缺陷软件定位；研究软件供应链成分分析技术和软件供应链上下游透明信息库构建技术；构建软件供应链安全分析与检测集成测试平台，进行试点应用。

考核指标：制定软件供应链安全管理的国家标准提案，覆盖软件的开发、交付、部署、升级等各个环节；建立软件产品和服务供应链组件智能识别与关系图谱分析系统和网络安全审查大数据平台原型系统，实现关联分析功能；软件成分分析精准率不低于 95%，依赖关系分析精准率不低于 90%；基于源代码可识别的开源组件数量不少于 300 万种，基于二进制代码可识别的软件组件数量不少 2000 种；已知缺陷存在性检测准确率不低于 95%，二进制代码识别准确率不低于 90%，基于二进制代码的已知缺陷检测准确率不低于 80%。

2.11 面向网络协同制造的工业协议安全测试技术

研究内容：研究面向工业协议的高效协议格式描述与解析方法，以及自动化安全测试引擎，支持工业协议的快速测试建模；

研究基于静态分析和主动学习的工业私有协议自动化逆向分析技术；研究算法级高效并行化技术，打破传统并行化技术中无法实现算法因子共享的壁垒，提高模糊测试的效率；研究工业协议主被动异常响应监测技术，设计面向协同通信状态的深度交互测试方法，研发面向工业协议的体系化智能安全测试平台，构建典型工业控制系统测试验证环境，开展应用验证。

考核指标：覆盖对 OPC UA、Modbus-RTU/TCP、Siemens S7、Ethernet/IP、EtherCAT、IEC104、IEC 61850、DeltaV、PKS、CS3000、MQTT 等不少于 50 种主流工业协议的安全模糊测试，支持协议快速测试建模；实现重要领域至少 5 种工业私有协议的自动化逆向分析，协议格式推断准确率不低于 80%、语义推断准确率不低于 70%；相较于 Peach 代码覆盖率提高 150%以上，相较于现有并行化技术，相同并行节点数条件下，效率提升 50%以上；完成不少于 20 种工业控制系统测试验证，完成至少 5 种工控系统协议栈异常监视模型，异常报警响应时间小于 1 秒，发现不少于 10 个协议漏洞。

2.12 大规模异构物联网威胁可控捕获与分析技术

研究内容：针对当前物联网被用做大规模僵尸网络、物联网本身异构多样带来的物联网设备漏洞百出，以及未知威胁未知攻击手法难以发现等问题，研究海量流量中物联网攻击行为发现和恶意代码捕获技术，研究攻击报文快速聚类与关联技术、研究恶意样本逆向分析与自动分类技术、研究物联网僵尸网络追踪与威

胁评估技术、多层控制物联网僵尸网络发现分析技术、研究零日漏洞利用行为发现与漏洞验证技术，构建一套大规模物联网威胁数据捕获与威胁信息抽取系统，提升物联网僵尸网络、未知威胁及攻击手法发现等能力，达到全面感知物联网攻击行为、全面捕获物联网威胁数据、全面提取物联网威胁信息、全面发现物联网未知威胁的效果。

考核指标：形成 1 套大规模物联网威胁数据捕获与威胁信息抽取系统；识别物联网攻击行为次数不少于 1 亿/日，捕获物联网恶意样本数量不低于 1000 万/年，恶意样本检测精度不低于 95%，恶意样本分类准确率不低于 90%；发现物联网攻击手法、漏洞利用等特征不低于 500 条；构建可控的物联网诱饵环境，主动引导黑客攻击，捕获高质量的原始攻击数据，降低误报率，发现未知的物联网家族不少于 2 个、发现物联网大型僵尸网络不少于 10 个，分析发现层数超过 2 层的物联网僵尸控制网络不少于 5 个；在 48 小时内进行全网探测评估僵尸网络影响范围；发现新型移动端 APT 跨越攻击手法，检测内网中物联网设备漏洞，发现和识别物联网的未知威胁（0-day 漏洞的在野利用）不少于 5 个。

2.13 面向网络协同制造的 B5G/6G 可信接入与服务安全

研究内容：针对 B5G/6G 协同制造场景下复杂业务环境和多元信任关系，解决终端设备可信接入和端到端安全能力不足的问题，满足协同制造业务差异化安全服务的需求。研究网络设备身份标识可信管理机制，形成行业终端可信接入与转发的安全模型，

支持 B5G/6G 网络的可信接入；研究 B5G/6G 网络中网络服务防护框架，研究持续安全评估及动态授权访问控制机制；研究跨网络域、跨硬件、软件安全层和跨不同网络分层的可信协作技术，保障网络功能的安全可信运行；研究细粒度的网络切片分级认证和授权机制，以及适用于动态切片和动态组网的安全服务和策略自适应技术；研究 B5G/6G 网络功能交互主动性安全机制，以及调用逻辑推理和关联智能化分析技术；研究自适应的网络安全功能柔性重组技术，实现安全、网络和计算等资源的按需动态重构，满足面向协同制造的 B5G/6G 多样化的安全需求。

考核指标：构建多维度、立体化、弹性网络安全防御技术框架，保障 B5G/6G 网络应对新型网络安全威胁；研发 B5G/6G 终端可信接入系统，实现面向设备真实性的随路验证和动态授权的网络服务访问控制，针对不同网络场景实现不少于 2 项自适应切片安全服务模型；研发面向 B5G/6G 的网络功能主动性异常检测系统，定位异常行为不少于 2 种，准确率不低于 80%；研发面向网络功能虚拟化的电信云原生安全防护系统，单虚机转发性能不低于 100Gbps，单虚机对称加解密性能不小于 100Gbps，转发时延不大于 20 微秒；申请发明专利不少于 10 项，至少形成一项行业标准提案，并结合协同制造场景，实现 B5G/6G 网络可信接入与服务安全系统的试验示范。

2.14 云边协同的工业智能控制器安全防护技术

研究内容：研究典型云边协同工业场景边缘智能控制平台安

全风险，设计基于控制交互机理与内生安全构造的主动安全防御模型；研究边缘终端设备协同控制、动态演进的规则映射机制，研究基于源代码和二进制的嵌入式控制平台安全漏洞模式和缺陷检测机制，设计可主动防御内部未知安全漏洞的系统架构，构建覆盖边缘智能控制平台开发、部署、运行和更新等全生命周期的主动安全防护机制；研发具备主动防御能力的智能工业控制系统原型，实现漏洞和缺陷检测、边缘通信保护、威胁识别、安全隔离、快速响应与补偿恢复，并在能源、电力、交通、制造等典型行业开展应用验证。

考核指标：提出覆盖全生命周期的工业互联边缘智能安全防护体系，研发 1 套智能工业控制系统原型，支持输入输出信号点 2 万点以上，支持至少 10 种典型工业协议，支持基于商用密码的身份认证、通信加密和数据完整性保护；建立边缘通信防护、威胁识别、隔离与响应算法/策略库，支持算法库/知识库不少于 5 类，支持安全漏洞模式不少于 20 种，源代码检测效率不低于 200 万行／小时；安全事件响应时间（攻击事件发现到报警/隔离时间）小于 200 毫秒；形成至少 1 项国家/行业标准提案；完成至少 3 个典型行业的应用验证。

2.15 道路交通系统大规模异构终端网络安全防护技术与应用

研究内容：研究道路交通系统异构终端的分级分类方法、标识数据结构及解析规范，构建道路交通运输行业标识解析体系；设计基于行业密钥、身份管理证书和国密算法芯片的安全访问控

制策略，构建道路交通系统海量异构终端的数字身份信任体系；从设备、数据、网络通信、接入等安全维度，构建覆盖设备层、网络层、平台层、应用层，贯穿道路交通系统全生命周期的自主可控深度安全防护体系；研发安全防护模块、安全管理系统、标识接入组件与装置；在道路交通系统重点场景开展规模化应用，形成具有示范意义的安全防护解决方案。

考核指标：针对道路交通系统重点场景的安全需求，构建能够覆盖设备层、网络层、平台层、应用层等各层次的安全防护体系，总体功能覆盖率不少于 95%；研发不少于 10 款主动标识安全接入终端支持接入道路运输业行业标识解析节点，支持国密二级、支持 SM2/3/4 算法，能够保障道路交通系统异构终端的数据、通信、身份等安全；在高速公路、城市道路中开展路况监测、应急管理、车辆调度等不少于 5 种典型场景的安全防护应用验证，接入安全终端数不低于百万级；申请发明专利不少于 10 项，形成行业标准提案不少于 2 项。

2.16 气象卫星业务测控及数据服务的安全关键技术

研究内容：研究气象卫星业务测控系统卫星控制指令可信生成、商用密码加密、多路径高可信传输等测控安全关键技术；研究气象卫星业务测控应用的动态访问控制、可信身份认证与权限管理、安全策略引擎等智能微边界防护关键技术；研究支持细粒度数据分级、动态授权、自验证、内生安全的气象卫星数据可信标识体系，研究面向多行业气象卫星数据服务可追溯、防篡改、

防滥用的全流程安全防护与精准管控技术；研究去中心化的气象卫星数据资产的责权界定、授权共享、价值交换等数据治理技术；研发气象卫星业务测控与数据服务安全综合防御系统，实现气象卫星关键业务系统的安全加固和服务监管。

考核指标：支持控制信道商用密码加密，支持多条路径传送指令，卫星指令发送100%安全准确；攻击检测规则不少于10万条，威胁情报不少于200万条，可对接第三方威胁情报不少于100亿条；支持可信标识服务，具备管理千亿级数据标识的能力，单个节点支持每秒10万次标识生成、可信验证，延迟低于1毫秒；气象卫星数据资产的数据治理支持千量级节点，每秒操作数不低于10000，单次操作确认时间不超过1分钟；提交气象卫星业务测控与数据服务安全技术体系研究报告1套；研发1套气象卫星业务测控与服务安全综合防御原型系统，支持卫星数量不低于5颗，支持10万级用户并发访问，系统运行成功率大于99.0%。

2.17 低空智联网安全管控与服务关键技术

研究内容：研究低空智联网安全协同管控策略，研究低空智联网的总体安全架构，形成安全管控技术标准体系；研究低空智联网信息采集、融合技术，研究空天地一体低空智联网安全态势感知与预测技术；研究低空智联网安全风险评估技术、ADS-B等无线入侵智能检测技术，研究低空智联网多维安全威胁检测、动态防御及管控技术；研究低空智联网跨域、多级信息安全保护与共享技术，航空器数据安全交换及验证技术，建立管控大数据安全共享机制；

研发低空智联网安全管控与服务平台并开展应用验证。

考核指标：制定低空智联网安全协同管控策略、构建低空智联网安全架构，形成 2~3 项行业标准提案；支持不少于 5 类设施设备接入、不少于 5 种多源动态飞行数据融合处理；具备有线和无线攻击入侵检测能力，检测率达到 95%以上；支撑安全管控与服务；在省域范围不少于 2 个典型应用场景应用示范，参与航空器不低于 1 万架次。

2.18 新一代水下系统的网络安全关键技术与应用示范

研究内容：研究面向大带宽高实时、复杂异构终端场景的可重构网络安全架构；针对多域多业务多安全等级融合访问安全问题，研究基于细颗粒度多层级身份认证和网络动态安全隔离防护技术；针对安全威胁渗透至信息物理系统，研究业务行为建模与深度分析学习技术；研究在不同场景、不同业务等级以及紧急状态下确保核心业务在网络中可信传输的系统安全功能按需重构技术；研究和构建测试环境并开发原型系统，开展应用示范。

考核指标：构建 1 套满足新一代水下系统的网络空间安全架构，覆盖身份认证、终端防护、隔离过滤、检测预警全面能力；构建 1 套满足新一代水下系统网络安全防护白皮书和相关行业标准提案；支持新一代水下系统大带宽网络场景下安全隔离技术，支持应用级、终端级、接入级和网络级隔离、会话层和指令层协议深度解析和实时阻断技术；支持基于物理机、虚拟机及容器的轻量化隔离防护技术，实现所有内部会话可视可管可控；支持网

络会话与未知指令的学习能力，未知指令解析与学习能力不低于50Mbps；支持安全交换一体化，网络交换能力不低于1Tbps，支持40G端口带宽，单跳时延不大于10微秒，实现网络安全一体化增强；支持智能安全管控态势，支持节点管控能力不低于1000个节点，支持至少10种内部安全事件分析与警报能力。

2.19 互联网信息推荐算法安全评估理论与方法

研究内容：基于用户属性和信息消费时空行为及内容分布等特征，研究信息推荐算法的用户行为画像、高分辨率用户群体划分、定向投放技术，支撑针对信息推荐算法及推荐内容的监控；研究基于用户群体画像的推荐系统诱导传播和定向控制技术，实现对推荐系统外部干扰的识别与利用；研究信息推荐算法安全评估量化指标体系，支撑对信息推荐算法的信息安全评估；研究信息推荐算法宏观治理方法，设计推荐算法安全运营基础性原则和要求细则，研制互联网信息推荐算法安全评估示范应用平台，支持推荐算法的良性创新与应用。

考核指标：建立至少5个维度的信息推荐算法安全要求和评价体系；实现至少40个以上信息推荐算法监测量化指标；在至少2个国内主流互联网媒体平台中，实现至少300万用户的高分辨率群体分类，其中必须包含未成年人、特殊行业从业人士等特殊重点监控群体；具备对至少10类重点用户群体的信息消费过程的实时监测和评估服务、以及对重点信息、正能量内容和有害信息在各人群中的传播情况进行监控；在不同群体内，

实现非偏好信息的诱导曝光，曝光率不低于 30%，并能够有效识别出被诱导曝光信息，识别准确率不低于 80%；研制互联网信息推荐算法安全评估示范应用平台，实现不少于 10 个互联网媒体信息推荐平台的算法动态安全评估，形成互联网信息推荐算法监管支撑能力。

“网络空间安全治理”重点专项
2022 年度项目申报指南形式审查条件要求

申报项目须符合以下形式审查条件要求。

1. 推荐程序和填写要求。

（1）由指南规定的推荐单位在规定时间内出具推荐函。

（2）申报单位同一项目须通过单个推荐单位申报，不得多头申报和重复申报。

（3）项目申报书（包括预申报书和正式申报书，下同）内容与申报的指南方向（榜单任务）相符。

（4）项目申报书及附件按格式要求填写完整。

2. 申报人应具备的资格条件。

（1）项目（课题）负责人应为 1962 年 1 月 1 日以后出生，具有高级职称或博士学位。

（2）青年科学家项目负责人应具有高级职称或博士学位，男性应为 38 周岁以下（1984 年 1 月 1 日以后出生），女性应为 40 周岁以下（1982 年 1 月 1 日以后出生）。原则上团队其他参与人员年龄要求同上。

（3）受聘于内地单位的外籍科学家及港、澳、台地区科学家可作为项目（课题）负责人，全职受聘人员须由内地聘用单位提供全职聘用的有效材料，非全职受聘人员须由双方单位同时提供

聘用的有效材料，并作为项目预申报材料一并提交。

（4）项目（课题）负责人限申报 1 个项目（课题）；国家科技重大专项、国家重点研发计划、科技创新 2030—重大项目的在研项目负责人不得牵头或参与申报项目（课题），课题负责人可参与申报项目（课题）。

（5）参与重点专项实施方案或本年度项目指南编制的专家，原则上不能申报该重点专项项目（课题）。

（6）诚信状况良好，无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

（7）中央和地方各级国家机关的公务人员（包括行使科技计划管理职能的其他人员）不得申报项目（课题）。

3. 申报单位应具备的资格条件。

（1）在中国大陆境内登记注册的科研院所、高等学校和企业等法人单位。国家机关不得作为申报单位进行申报。

（2）注册时间在 2021 年 6 月 30 日前。

（3）诚信状况良好，无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

4. 本重点专项指南规定的其他形式审查条件要求。

青年科学家项目不再下设课题，项目参与单位总数不超过 3 家。

本专项形式审查责任人：刘英军